警察情報管理システム運用管理要領の制定について

平成２５年４月１日
例規（情管）第２２号
警　察　本　部　長

〔沿革〕平成２６年７月例規（情管）第４２号　平成２６年12月例規（情管）第７４号

各部長・参事官・所属長

見出しの要領を別添のとおり制定し、平成２５年 ４ 月 １ 日から実施することとしたので、誤りのないようにされたい。

なお、千葉県警察情報管理システム運用要領の制定について（平成２０年例規（情管）第４７号）は、廃止する

別添

警察情報管理システム運用管理要領

第１　総則

１　趣旨

この要領は､警察情報管理システムのシステム設計及び運用並びに維持管理に関し、必要な事項を定めるものとする。

２　用語の定義

この要領における用語の意義は、次に掲げるもののほか、警察情報管理システムの運用管理に関する訓令（平成２５年本部訓令第８号）における用語の例による。

（１）ソフトウェア　電子計算機を動作させるためのプログラム及びこれに付随するデータの総称をいう。

（２）千葉県警察情報管理システム最適化計画　千葉県警察全体のシステムの費用対効果を高め、かつ、効果的な整備を行うための統一的なシステム整備計画をいう。

（３）メールボックス　電子メールシステムにおけるユーザ固有の使用領域をいう。

（４）共有キャビネット　電子メールシステムにおいて、ユーザがお互いのデータを共有するための保存領域をいう。

（５）ファイルサーバ　ユーザに対して記憶装置の機能を提供する電子計算機及びプログラムをいう。

（６）個人キャビネット　ファイルサーバに確保する個人用保存領域をいう。

（７）所属フォルダ　ファイルサーバに確保する所属用保存領域をいう。

（８）文書等　ワープロソフト、表計算ソフト等で作成した電磁的文書、ホームページ（ポータルサイトを除く。）等をいう。

（９）ポータルサイト　業務系システムにおいて、業務に必要な文書等を集中して掲載するホームページをいう。

（１０）アプリケーションソフト　ワープロソフト、表計算ソフト等のソフトウェアを

いう。

（１１）アクセスログ　アクセスに関する記録をいう。

（１２）ｂｃｃ（ブラインドカーボンコピー）　同一の電子メールを複数の利用者に送信するときに、受取人本人以外のメールアドレスを隠したまま送信する機能をいう。

（１３）認証情報　ユーザＩＤ、パスワード、個人に特有の生体的特徴、その他のアクセス権者を識別又は検証するための情報をいう。

（１４）認証用媒体　認証情報を記録した媒体をいう。

（１５）個人情報　個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む。）をいう。

（１６）個人情報入力資料　個人情報が記載され、又は個人情報が電磁的方法により記録された入力資料をいう。

（１７）個人情報出力資料　個人情報が記載され、又は個人情報が電磁的方法により記録された出力資料（警察職員又は警察職員であった者に係る出力資料であって、専らその人事、給与若しくは福利厚生に関する事項又はこれらに準ずる事項を記録するものを除く。）をいう。

第２　準拠

警察情報管理システムのシステム設計及び運用並びに維持管理については、別に定める場合を除き、この要領の定めるところによる。

第３　細目的事項に関する委任

この要領に定めるもののほか、警察情報管理システムのシステム設計及び運用並びに維持管理に関して必要な細目的事項は、対象業務の主管部長が定めるものとする。

なお、必要によりシステム責任者に意見を求めるものとする。

第４　所属における管理体制

１　運用管理者

（１）所属に運用管理者を置き、所属長をもって充てる。

（２）運用管理者は、所属における警察情報管理システムによる処理に係る個人情報の適正な取扱い並びに警察情報管理システムの適正な運用及び維持管理に関する事務を統括する。

２　運用副管理者

（１）所属に運用副管理者を置き、次長（ただし、警備部成田国際空港警備隊は総務室長）をもって充てる。

（２）運用副管理者は、運用管理者の命を受け、所属における警察情報管理システムによる処理に係る個人情報の適正な取扱い並びに警察情報管理システムの適正な運用及び維持管理に関する事務を処理する。

３　ＯＡ取扱責任者及びＯＡ取扱補助者

（１）所属にＯＡ取扱責任者及びＯＡ取扱補助者を置き、次表に掲げる者をもって充てる。

区　　分	県 本 部	署			
			幹部交番	交　　番	駐 在 所
ＯＡ取扱責任者	課 長 補 佐	各課長	幹部交番所長		
ＯＡ取扱補助者	各係の長（特別の理由がある場合は、適性を有する主任を運用管理者が指定することができる。また、係長又は主任の配置がない場合は、適性を有する係員の中から指定する。）	左　同	左　同	交番所長又は係長（特別の理由がある場合は、適性を有する主任を運用管理者が指定することができる。）	駐在所勤務員

（２）課長補佐の配置がない場合は、警部（相当職を含む。）以上の階級にある直属の上司をＯＡ取扱責任者に指定するものとする。

（３）複数の所属の職員が一時的に集合して業務を行う必要がある場合には、当該業務に関して、主たる責任を有する運用管理者が警部（相当職を含む。）以上の階級にある者の中からＯＡ取扱責任者を指定するものとする。

（４）ＯＡ取扱責任者は、運用副管理者を補佐するものとする。

（５）ＯＡ取扱補助者に主任又は係員を指定した場合は、所属内で名簿を作成するなど、管理体制を明らかにするとともに、システム責任者へ報告すること。

（６）ＯＡ取扱補助者は、ＯＡ取扱責任者の指示を受けてその任務を補助するものとする。

４　ＯＡ取扱指導者

（１）所属にＯＡ取扱指導者を置くものとする。

（２）ＯＡ取扱指導者は、情報処理能力検定上級取得者その他適性を有する職員の中から次表の指定基準により運用管理者が指定するものとする。

県 本 部	署	
		幹部交番
庶務係を含む１人以上（分室等がある場合は、分室ごとに１人以上）	各課１人以上	１人以上

（３）ＯＡ取扱指導者は、警察情報管理システムの運用について、職員の指導に当たるものとする。

なお、ＯＡ取扱補助者を兼務することを妨げない。

第５　千葉県警察情報管理システム最適化計画の推進等

１　システム統合基盤の整備

システム総括責任者は、システムを新設又は変更する場合は、千葉県警察情報管理システム最適化計画との整合性を検討しなければならない。

２　統一的システム構築の確立

（１）運用主管課長は、新たに対象業務を運用するために必要なシステムを導入しよう

とする場合は、事前に情報管理システム最適化計画の推進に関する事前協議申請書（別記第１号様式）により、システム責任者と事前協議するものとする。

（２）システム責任者は、既存システム、その他検討段階のシステムとの連携等について十分検討した上で、当該運用主管課長と協議し、必要な助言を行うものとする。

３　千葉県警察情報管理システム最適化計画の詳細

千葉県警察情報管理システム最適化計画の詳細については、システム総括責任者が別に定めるものとする。

第６　対象業務の新設等の申請

１　対象業務新設の申請

（１）運用主管課長は、前第５の２の協議の結果、対象業務の新設が必要であると認められるものについては、対象業務新設申請書（別記第２号様式）により、システム責任者を経由してシステム総括責任者に申請するものとする。

（２）システム総括責任者は、前（１）の申請があった場合はこれを審査し、適当と認めるときは、対象業務に指定するものとする。

２　対象業務変更の申請

（１）運用主管課長は、対象業務の変更が必要であると認めたときは、システム責任者と事前協議をした上で、対象業務変更申請書（別記第３号様式）により、システム責任者に申請するものとする。

（２）システム責任者は、前（１）の申請があった場合はこれを審査し、適当と認めるときは、対象業務を変更するものとする。

３　対象業務指定解除の申請

（１）運用主管課長は、対象業務の廃止が必要であると認めたときは、システム責任者と事前協議をした上で、対象業務指定解除申請書（別記第４号様式）により、システム責任者を経由してシステム総括責任者に申請するものとする。

（２）システム総括責任者は、前（１）の申請があった場合はこれを審査し、適当と認めるときは、対象業務の指定を解除するものとする。

第７　対象業務の実施方法の策定等

１　実施方法の策定

運用主管課長は、その所管に属する対象業務について、次（１）から（５）までの事項のほか、対象業務の特性を踏まえ、必要に応じて（６）から（１０）までの事項を、前第６の方法により申請し、システム総括責任者の承認を得た上で定めなければならない。

なお、警察庁情報管理システムによる対象業務については、警察庁の運用主管課長が定める事項を踏まえ、策定するものとする。

（１）対象業務の目的に関する事項

（２）対象業務の運用の体制に関する事項

（３）対象業務において利用するファイルに関する事項

（４）対象業務における登録、照会等の手順に関する事項

（５）対象業務に係るアクセス範囲に関する事項

（６）対象業務に係る入力資料及び出力資料の取扱いに関する事項

（７）個人情報照会（個人情報を対象とする照会をいう。以下同じ。）に関する記録の確認方法に関する事項
（８）対象業務に係る部外への委託に関する事項
（９）対象業務に係る取扱説明書の取扱いに関する事項
（１０）その他対象業務の適正かつ円滑な実施に必要な事項

２　実施方法の周知及び指導

（１）運用主管課長は、前１により策定する対象業務の実施方法を関係職員に周知しなければならない。
（２）運用主管課長は、関係職員に対して対象業務が適正かつ円滑に行なわれるよう、その実施方法について適切に指導しなければならない。

第８　運用等

１　運用時間

警察情報管理システムは、原則として２４時間運用とする。

２　電子メール等の利用

（１）目的

電子メールは、職員相互及び全国の警察職員並びに部外との事務連絡や文書等の送受信に利用することを目的として設定する。

（２）ユーザＩＤの交付等

ア　システム総括責任者は、原則として、所属の分掌単位にユーザＩＤを交付するものとする。
イ　運用管理者は、電子メール又は共有キャビネットを利用する分掌が新たにできるとき及び分掌名が変更又は廃止されるときは、ユーザＩＤ交付（廃止）申請書（別記第５号様式）によりシステム責任者を経由してシステム総括責任者に申請するものとする。

（３）電子メールの利用上の留意点

ア　電子メールの本文は、原則としてテキスト形式とする。
イ　職員は、電子メールの内容（添付ファイルを含む。）を十分精査し、疑義を生じるおそれのある事項の排除に努めなければならない。
ウ　電子メールに添付するファイルの容量は、必要最小限とする。
エ　職員は、メールボックスを随時点検し、不要な警察情報の削除に努めなければならない。
オ　情報系システムによる部外との電子メールの利用に係る特記事項については、次記５（３）に示すとおりとする。

（４）共有キャビネット等の利用

次３（３）と同様の扱いとする。

３　ファイルサーバの運用

（１）情報を保存する必要性

運用管理者は、ファイルサーバに保存する情報について、その必要性を次表等により勘案した上で保存し、又は削除するものとする。また、これに限らず、不要となった情報については速やかに削除するなど、ファイルサーバの適正かつ効果的な

運用に努めなければならない。

保存できる情報	保存できない情報	削除すべき情報
○　職務上の情報と認められるもの ○　現在及び将来において有効活用できると認められるもの	○　私事案件に関するもの ○　明らかに現在及び将来において有効活用できないと認められるもの	○　行政文書としての保存期間が経過したもの ○　相当の長期間にわたって使用していない古い情報と認められるもの

（２）個人キャビネットの利用

ア　職員は、業務を遂行する上で必要な情報のうち、職員個人が業務系システム上で利用する警察情報を個人キャビネットに保存することができるものとする。

イ　ＯＡ取扱責任者は、ポータルサイト上の「アクセス権管理システム」により、部下職員の個人キャビネットの使用状況を、必要に応じて点検するものとする。

（３）所属フォルダの利用

職員は、他の職員が閲覧又は利用しても支障のない情報を所属フォルダに保存することができるものとする。

なお、特定のグループに限定して閲覧又は利用する情報については、自己復号型暗号化（パスワード設定）機能等を活用して同グループが管理するパスワードを設定し、保存するものとする。

４　ポータルサイトの利用

（１）文書等の掲載申請

運用管理者は、ポータルサイトに文書等の掲載を希望するときは、システム責任者と事前協議した上で、ポータルサイト利用（掲載・削除）申請書（別記第６号様式)によりシステム責任者を経由してシステム総括責任者に申請を行うものとする。

（２）文書等の掲載基準

運用管理者は、ポータルサイトに掲載しようとする文書等が次のアからウまでの基準を満たしていることをあらかじめ確認しなければならない。

ア　警察業務を遂行するために必要であること。

イ　アプリケーションソフトで作成した文書等については、当該文書等がコンピュータ・ウイルスに感染していないことを確認したものであること。

ウ　ポータルサイトに掲載する文書等のデータの容量は、１ファイル当たり原則として３メガバイト以内とすること。

（３）掲載する文書等の作成

ポータルサイトに掲載する文書等の作成は、掲載所属が行うものとする。

（４）文書等の掲載及び更新

ア　前記（１）の申請に基づく文書等の掲載は、システム責任者が行うものとする。

イ　ポータルサイト上の文書等の更新は、当該文書等の掲載を申請した所属が行うものとする。

なお、システム責任者は、文書等の更新を担当する職員が、同作業を行えるよ

う必要な措置を講ずるものとする。

（５）掲載文書等の管理

ア　運用管理者は、ポータルサイトに掲載する文書等の容量が必要最小限となるよう努めなければならない。

イ　システム責任者は、ポータルサイトに掲載された文書等の総量が警察情報管理システムの運用に支障を及ぼすおそれがあると判断した場合には、当該運用管理者に、掲載した文書等の整理を求めることができるものとする。

ウ　文書等は、原本の保存期間を超えて掲載してはならない。

（６）掲載文書等の削除

ア　運用管理者は、ポータルサイトに掲載した文書等の削除を希望するときは、ポータルサイト利用（掲載・削除）申請書によりシステム総括責任者に申請するものとする。

イ　運用管理者は、常にポータルサイトの利用状況を把握し、掲載基準を満たさない文書等を認めたときは、前アにより速やかに削除の申請を行うものとする。

ウ　システム責任者は、ポータルサイトにおいて掲載基準を満たさない文書等を認めたときは、当該運用管理者に文書等の削除の申請を求めるものとする。

エ　ポータルサイトに掲載する文書等の削除は、システム責任者が行うものとする。

５　情報系システムの運用に係る留意事項

（１）情報の管理

ア　端末装置に内蔵されたハードディスクに警察情報を保存してはならない。

イ　千葉県警察情報セキュリティに係る管理要領の制定について（平成２６年例規（情管）第７０号。以下「管理要領例規」という。）第１の２に規定する「機密性高情報」及び「機密性中情報」は、原則として取り扱ってはならない。

（２）インターネットの利用

ア　ホームページの閲覧等

職員は、次の（ア）から（ウ）までの事項を厳守しなければならない。

（ア）警察業務以外の目的でインターネットを利用しないこと。

（イ）情報料が必要となるもの又はインターネット上の掲示板への書込み等のインターネットサービスは、原則として利用しないこと。

（ウ）安全性の確認ができない、又は違法性が高いホームページ等は、原則として閲覧しないこと。

イ　アクセスログの検証

システム責任者は、インターネットに係るアクセス状況及びダウンロードしたファイルの一覧を定期的に確認するものとし、何らかの疑いのある使用状況が確認されたときは、運用管理者に通知し、使用実態の調査その他の必要な措置を求めるものとする。

（３）部外との電子メールの利用

ア　職員は、警察業務以外の目的で部外との電子メールを利用してはならない。

イ　職員は、原則として管理要領例規第１の２に規定する「機密性低情報」に限り、部外との間で送受信することができる。この場合において、電子メールの本文等

に、当該情報が一般に公開しても差し支えのない情報である旨を明記しなければならない。

なお、「機密性中情報」を部外との間で送受信しようとするときは、運用管理者の許可を得なければならない。

ウ　前イの許可に係る事務については、ＯＡ取扱責任者に委任することができるものとする。

エ　職員は、電子メールを送信するときは、誤送信に十分注意しなければならない。特に、複数の相手に一斉送信する際、受信者が互いの送信先メールアドレスを知る必要がないときは、「ｂｃｃ」欄に送信先メールアドレスを設定の上、送信すること。

オ　職員は、差出人不詳又は覚えのない電子メールを展開してはならない。

カ　ＯＡ取扱責任者は、電子メールの送受信記録を随時確認し、不正使用等の予防に努めなければならない。

キ　システム責任者は、電子メールの送受信記録を定期的に確認するものとし、何らかの疑いのある使用状況が確認されたときは、運用管理者に通知し、使用実態の調査その他の必要な措置を求めるものとする。

第９　アクセス権の付与等

１　アクセス権の申請

運用管理者は、職員にアクセス権を付与する必要がある場合は、対象業務を行う上で必要なアクセス範囲に限定し、運用主管課長を経由してシステム総括責任者にアクセス権の付与の申請を行うものとする。

２　アクセス権の付与

システム総括責任者は、前１の申請に基づき、必要と認める場合は、アクセス権を付与するものとする。

第１０　認証情報の管理等

１　認証情報の管理

システム総括責任者は、警察情報管理システムに登録された認証情報を適切に管理しなければならない。

２　アクセス権者の責務

（１）認証用媒体の管理等

認証用媒体を利用するアクセス権者は、自己の認証用媒体により他人にアクセスをさせ、又は他のアクセス権者の認証用媒体を用いてアクセスをしてはならない。

（２）ユーザＩＤの管理等

ユーザＩＤを利用するアクセス権者は、自己のユーザＩＤにより他人にアクセスをさせ、又は他のアクセス権者のユーザＩＤを用いてアクセスをしてはならない。

（３）パスワードの管理

パスワードを利用するアクセス権者は、パスワードを定期的に変更するなど、他人にパスワードを知られることがないようにしなければならない。

３　アクセスに関する記録等

（１）アクセスに関する記録

システム総括責任者は、警察情報管理システムを構成するサーバ等に対するアクセスの日時及び内容並びに当該アクセスを行ったアクセス権者の氏名又はユーザＩＤを電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。以下同じ。）により記録しておかなければならない。

（２）アクセスに関する記録の保存

システム総括責任者は、前（１）の規定による記録を当該記録をした日から起算して５年以上保存しておかなければならない。

（３）アクセスに関する確認

システム総括責任者は、システム責任者に前記（１）の規定による記録を点検させ、アクセスが適正に行われたか否かを確認するものとする。

４　個人情報照会に関する記録等

（１）個人情報照会に関する記録

システム総括責任者は、個人情報照会の日時、目的、内容及び当該個人情報照会を行った者の氏名（職員の職員番号その他当該照会者を識別できる符号を含む。以下同じ。）を電磁的方法により記録しておかなければならない。

（２）個人情報照会に関する記録の保存

システム総括責任者は、前（１）の規定による記録を当該記録がされた日から起算して５年以上保存しておかなければならない。

（３）個人情報照会に関する確認

ア　運用主管課長は、対象業務において利用する情報の機密性に鑑み、第７の１の規定により、必要に応じて前記（１）及び（２）の規定により保存される個人情報照会の記録の確認方法を定めるものとする。

イ　システム総括責任者は、前記（１）及び（２）の規定による記録に基づき、必要に応じて個人情報照会が適正に行われたか否かを確認するものとする。

第１１　個人情報入力資料の取扱い

１　個人情報入力資料の作成等

個人情報入力資料の作成及び個人情報入力資料に記載され、又は記録された情報に係る警察情報管理システムへのデータの入力は、対象業務主管課及び端末装置の設置された運用所属において対象業務の目的に従いあらかじめ定められた手続により正確に行うこと。ただし、特別の理由がある場合は、入力資料依頼書（別記第７号様式）によりシステム責任者にデータの入力を依頼することができるものとする。

２　個人情報入力資料の交付

（１）個人情報入力資料は、対象業務の目的に従いあらかじめ定められた職員以外の者にこれを交付してはならない。

（２）個人情報入力資料の交付を送付の方法により行うときは、運用管理者は、職員にこれを携行させなければならない。ただし、職員にこれを携行させることが困難である場合において運用管理者が特に認めたときは、逓送又は書留郵便により送付することができる。

（３）システム責任者及び運用管理者が特に認めたときは、個人情報入力資料の交付を送信の方法（ファックス等）により行うことができる。

３　用済み後の個人情報入力資料の取扱い

（１）個人情報入力資料は、用済み後速やかにこれを返却し、又は廃棄（電磁的方法により記録された個人情報の場合は削除）しなければならない。

（２）個人情報入力資料の廃棄は、裁断、焼却等の復元できない方法により行わなければならない。

４　個人情報入力資料の保管

書面又は外部記録媒体である個人情報入力資料を保管する場合は、施錠のできる所定の保管庫等を用いて保管しなければならない。

５　個人情報入力資料の複写

（１）個人情報入力資料は、これを複写してはならない。ただし、対象業務を行うため複写する必要があるとしてシステム総括責任者が承認した場合は、個人情報入力資料を複写することができる。

（２）個人情報入力資料を複写した物は、個人情報入力資料とみなして前記２から次記６までの規定を適用する。

６　個人情報入力資料の交付等に関する記録

（１）運用管理者は、個人情報入力資料の交付、受入れ、保管、複写、返却又は廃棄（電磁的方法により記録された個人情報の場合は削除）（次記（３）において「交付等」という。）の日時及び目的、当該個人情報入力資料を取り扱った職員の氏名並びに当該個人情報入力資料の概要及び数量を入力資料管理簿（別記第８号様式）に記載し、又はこれらの事項を電磁的方法により記録しておかなければならない。

（２）運用管理者は、入力資料の受け払いが４回以上にわたるときは、入力資料管理補助簿（別記第９号様式）に処理状況を記録させておかなければならない。

（３）システム責任者及び運用管理者は、入力資料管理簿又はその電磁的記録に基づき、個人情報入力資料の交付等が適正に行われたか否かを確認しなければならない。

第１２　個人情報出力資料の取扱い

１　個人情報出力資料の作成

個人情報出力資料は、次に掲げる場合を除き、これを作成してはならない。

（１）対象業務の目的に従いあらかじめ定められた手続により作成するとき。

（２）次記４（１）イの規定により個人情報出力資料を交付するために作成するとき。

（３）警察情報管理システムの保守又は試験を行うため作成するとき。

（４）次記７の規定により、臨時的な出力に係る手続により作成するとき。

２　用済み後の個人情報出力資料の取扱い

前記第１１の３に定める用済み後の個人情報入力資料の取扱いに準ずるものとする。

３　個人情報出力資料の保管

前記第１１の４に定める個人情報入力資料の取扱いに準ずるものとする。

４　個人情報出力資料の交付

（１）個人情報出力資料は、次に掲げる場合を除き、これを交付（出力資料を取り扱う職員から、その他の者に対して当該資料又は当該資料に記録された情報を提供することをいう。以下同じ。）してはならない。

ア　法令の規定により交付を求められ、又は交付することが許されている場合にお

いて、システム総括責任者の承認を得て交付するとき。

イ　対象業務の目的に従いあらかじめ定められた者に交付するとき。

ウ　警察情報管理システムの保守又は試験のため交付する必要がある者に交付するとき。

エ　次記７の規定により、臨時的な出力に係る手続により作成し、交付するとき。

（２）個人情報出力資料を交付するときは、運用管理者は、当該個人情報出力資料が交付の目的以外の用に供されないよう適切にこれを管理するとともに、用済み後は、これを返却し、又は廃棄（電磁的方法により記録された個人情報の場合は削除）しなければならない。

（３）書面又は外部記録媒体である個人情報出力資料の交付を送付の方法により行うときは、運用管理者は、職員にこれを携行させなければならない。ただし、職員にこれを携行させることが困難である場合において運用管理者が特に認めたときは、逓送又は書留郵便により送付することができる。

（４）個人情報出力資料の交付を通信の手段により行うときは、その手段としてファイルサーバ、電子メール又はファクシミリを使用するものとし、交付又は受入れを行う所属の運用管理者は、対象業務ごとに交付又は受入れを担当する職員（以下「交付等担当者」という。）を指定するとともに、その手段ごとに次に掲げる事項を遵守しなければならない。ただし、システム総括責任者及び運用主管課長が特に認めた場合は、これによらない方法で交付することができる。

ア　ファイルサーバを使用する場合

（ア）電子計算機の指定

対象業務を行う上で必要な範囲において交付又は受入れに使用する電子計算機を指定（交番、駐在所等に設置される電子計算機は除く。）するとともに、指定した電子計算機以外の電子計算機で交付又は受入れを行う個人情報出力資料を取り扱わないようにしなければならない。

（イ）作成する共有フォルダへのアクセスの制限

運用管理者の所属及び対象業務ごとの共有フォルダを作成し、当該対象業務に係る交付等担当者以外の者がアクセスできないよう技術的な措置を講じなければならない。

（ウ）交付する資料の暗号化

前（イ）の規定により作成する共有フォルダに個人情報出力資料を保存する場合は、パスワードを利用して暗号化させるとともに、当該パスワードを交付等担当者以外の者に知られないようにしなければならない。

（エ）交付又は受入れ後の資料の削除

個人情報出力資料を交付し、又は受け入れた後は、前記（イ）の規定により作成する共有フォルダから速やかにこれを削除しなければならない。

イ　電子メールを使用する場合

（ア）電子メールの限定

交付又は受入れに使用する電子メールは、メールサーバにおいて送受信の履歴が収集でき、かつ、警察機関の内部に閉じた電気通信回線を使用するものに

限定しなければならない。

（イ）電子計算機の指定

対象業務を行う上で必要な範囲で交付又は受入れに使用する電子計算機を指定（交番、駐在所等に設置される電子計算機は除く。）するとともに、指定した電子計算機以外の電子計算機で交付又は受入れを行う個人情報出力資料を取り扱わないようにしなければならない。

（ウ）交付する情報の暗号化

交付する個人情報出力資料は、パスワードを利用して暗号化させるとともに、当該パスワードを交付等担当者以外の者に知られないようにしなければならない。

（エ）交付又は受入れ後の資料の削除

個人情報出力資料を交付し、又は受け入れた後は、送信用又は受信用のメールサーバから速やかにこれを削除しなければならない。

（オ）誤送信防止

交付先のメールアドレスを事前に登録しなければならない。

ウ　ファクシミリを使用する場合

（ア）交付する個人情報出力資料の限定

ファクシミリにより交付する個人情報出力資料は、次に掲げるものに限定しなければならない。

ａ　照会記録資料（個人情報照会に関する記録事項の通知資料をいう。）

ｂ　重要犯罪、重要窃盗犯、薬物・銃器犯罪及びひき逃げ事件の捜査並びに逮捕事件の送致等の事案であって、これらの事案処理のため緊急に必要となる個人情報出力資料

（イ）使用するファクシミリの指定

対象業務を行う上で必要な範囲で交付又は受け入れに使用するファクシミリ（送受信の履歴が収集できるものに限る。）を指定（交番、駐在所等に設置されるファクシミリは除く。）しなければならない。

（ウ）誤送信防止

ａ　前（イ）の規定により指定した交付に使用するファクシミリについては、一般加入回線への発信を停止した警察電話回線に接続するとともに、原則として、事前に交付先のファクシミリの番号を登録し、又は短縮ダイヤルを設定しなければならない。

ｂ　ファクシミリの使用に当たっては、この要領に定めるほか、千葉県警察の文書に関する訓令（平成２０年本部訓令第２２号）及び別に定める手続を遵守しなければならない。

（エ）交付等担当者の相互の連絡

交付先のファクシミリにおいて個人情報出力資料を受信した後、交付等担当者が速やかにこれを受領するよう、交付等担当者の相互の連絡を緊密に行わなければならない。

（オ）メモリ送信及びメモリ受信

メモリ送信の機能は利用させてはならない。また、ファクシミリが用紙切れ等によりメモリ受信した場合は、記録内容を印字した後、当該記録がメモリから削除されていることを確認しなければならない。

5　個人情報出力資料の複写

（1）個人情報出力資料は、次に掲げる場合を除き、これを複写してはならない。

ア　対象業務を行う上で複写する必要があるものとして運用管理者が認める場合

イ　警察情報管理システムの保守又は試験のため複写する必要がある場合

（2）前（1）の規定により個人情報出力資料を複写した物は、個人情報出力資料とみなして前記2から次記6までの規定を適用する。

6　個人情報出力資料の作成等に関する記録

（1）運用管理者は、個人情報出力資料の作成、交付、受入れ、複写、返却又は廃棄若しくはこれに電磁的方法により記録された個人情報の削除（次記（3）において「作成等」という。）の日時、目的、当該個人情報出力資料を取り扱う職員の氏名、当該個人情報出力資料の概要及び数量を出力資料管理簿（別記第１０号様式）に記載し、又はこれらの事項を電磁的方法により記録しておかなければならない。

（2）運用管理者は、前（1）の簿冊を最終の記載がされた日から5年以上保存し、又は前（1）の規定による記録を当該記録がされた日から5年以上保存しておかなければならない。

（3）運用管理者は、出力資料管理簿又はその電磁的記録に基づき、個人情報出力資料の作成等が適正に行われたか否かを確認しなければならない。また、システム総括責任者は、出力資料管理簿又はその電磁的記録に基づき、必要に応じ、個人情報出力資料の作成等が適正に行われたか否かを確認するものとする。

7　臨時出力資料の作成

（1）運用管理者は、対象業務について臨時に出力資料を必要とする場合は、臨時出力申請書（別記第１１号様式）により、運用主管課長に出力を申請するものとする。

（2）運用主管課長は、出力の申請があり、その必要があると認める場合又は自ら臨時出力を行おうとする場合は、臨時出力申請書により、システム責任者に申請するものとする。

（3）システム責任者は、運用主管課長に前（2）の臨時出力の対応の可否及び交付の方法を連絡するものとする。

なお、臨時出力資料を通信の手段により交付する場合は、業務系システムにより暗号化し、運用主管課長に送付するものとする。

（4）臨時出力資料を受領した運用主管課長は、これを前記第１１の4に定めるところにより、適正に管理しなければならない。

第１３　ドキュメント等の取扱い

1　ドキュメント等の交付

システムドキュメント及びプログラム並びに取扱説明書（以下「ドキュメント等」という。）は、これを対象業務に関係のない者に交付してはならない。

2　ドキュメント等の亡失等の防止

（1）システムドキュメント及びプログラム

システムドキュメント及びプログラムは、その亡失若しくは毀損又はこれに記載され、若しくは記録された警察情報管理システムの安全上秘密を要する事項の漏えいのないよう、運用管理者は、資料の名称、作成、交付、受入れ、複写、返却、保管、廃棄等管理の状況をドキュメント等管理台帳（別記第１２号様式）に記載し、又はこれらの事項を電磁的方法により記録するとともに、当該ドキュメント等が書面又は外部記録媒体の場合は、施錠のできる所定の保管庫等を用いて保管しなければならない。

（２）取扱説明書

警察情報管理システムの安全上秘密を要する事項が記載され、若しくは記録されているなど特に管理が必要なものとして、前記第７の１（９）の規定により運用主管課長が定める取扱説明書については、運用管理者は、資料の名称、交付、受入れ、複写、返却、保管、廃棄等管理の状況をドキュメント等管理台帳に記載し、又はこれらの事項を電磁的方法により記録するとともに、当該説明書が書面又は外部記録媒体の場合は、施錠できる所定の保管庫等を用いて保管しなければならない。

第１４　安全の確保

１　端末装置の設置場所

警察情報管理システムの端末装置は、対象業務に関係のない第三者がそのディスプレイ等に表示された内容を容易に見ることができない状態にしなければならない。

２　職員以外の者への業務の委託

対象業務の一部、警察情報管理システムを構成するサーバ等又は端末装置の保守若しくは試験等警察情報管理システムに関する業務を職員以外の者に委託する者は、次に掲げるところによりこれを行わなければならない。

（１）あらかじめ当該委託に係る業務の実施の場所及び方法、当該委託に係る業務に従事する者（以下「委託先担当者」という。）の範囲、個人情報又は警察情報管理システムの安全上秘密を要する事項の漏えいを防止するために執るべき措置等を明確に定めた特約を締結すること。

（２）委託先担当者にアクセスを行う権限を貸与する場合は、業務上必要な範囲に限定するとともに、当該委託先担当者による個人情報照会に関する記録を随時確認するなど､警察情報管理システムの不正な利用を防止するために必要な措置を執ること。

（３）委託先担当者が取り扱う個人情報入力資料又は個人情報出力資料の廃棄（電磁的方法により記録された個人情報の場合は削除）に当たっては、その状況を職員に確認させるなど、当該資料の不正な利用を防止するために必要な措置を執ること。

３　情報セキュリティの維持

警察情報管理システムの情報セキュリティの維持に関して実施する運用上の対策、技術的な対策その他の事項については、この要領に定めるもののほか、千葉県警察情報セキュリティに関する訓令（平成１６年本部訓令第５号）及びこれに基づいて定められる規程による。

以下様式省略